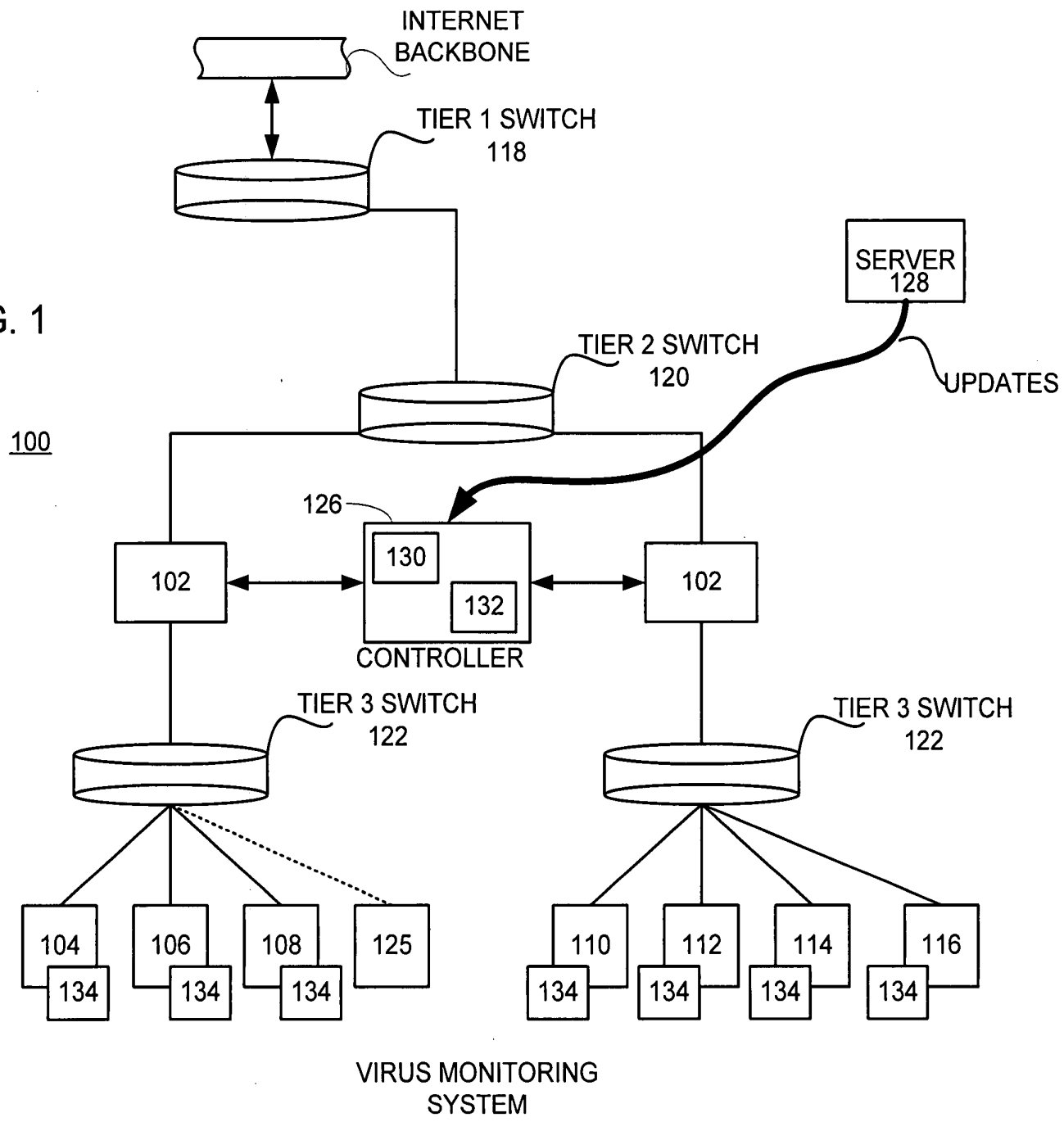
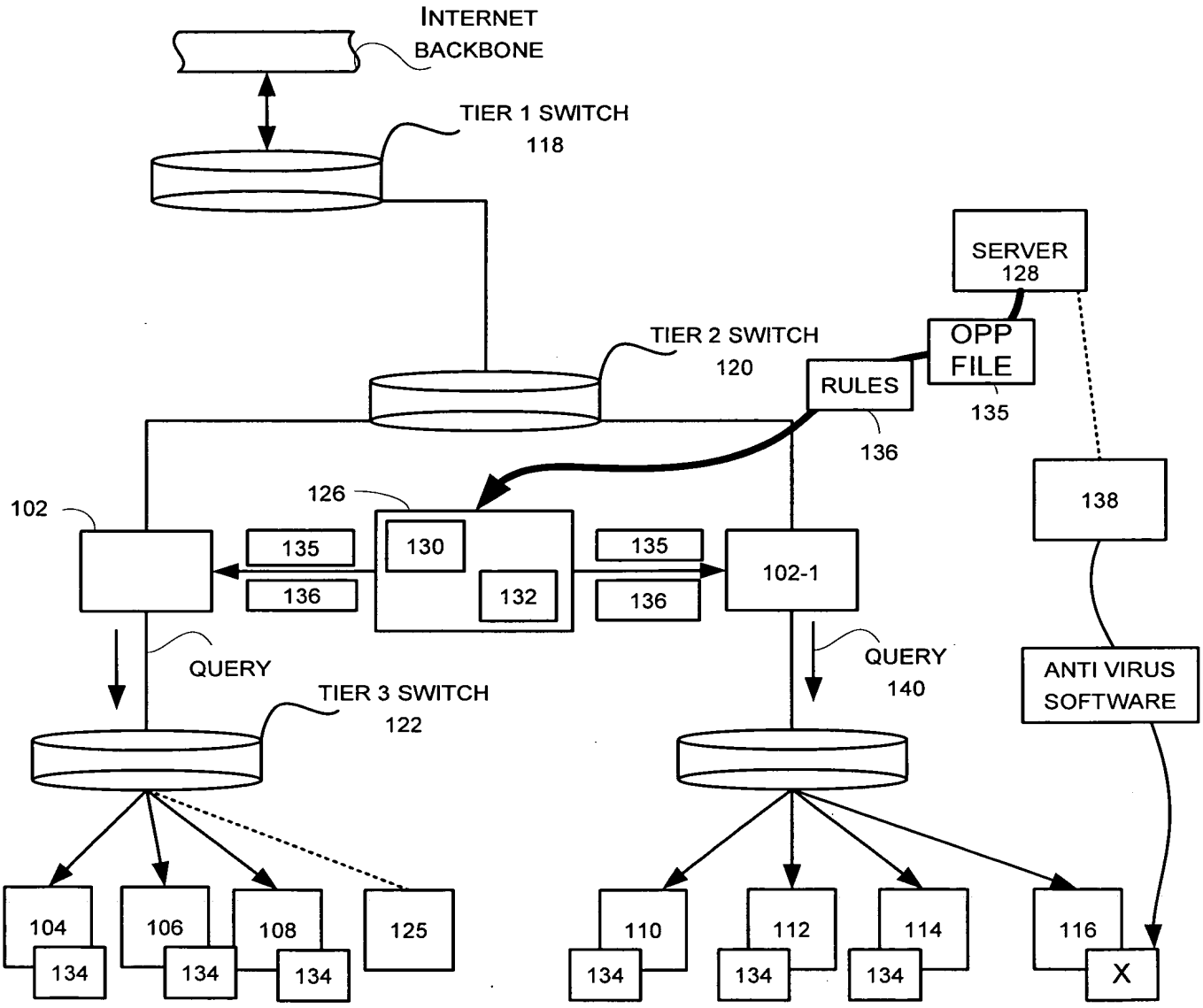
FIG. 1

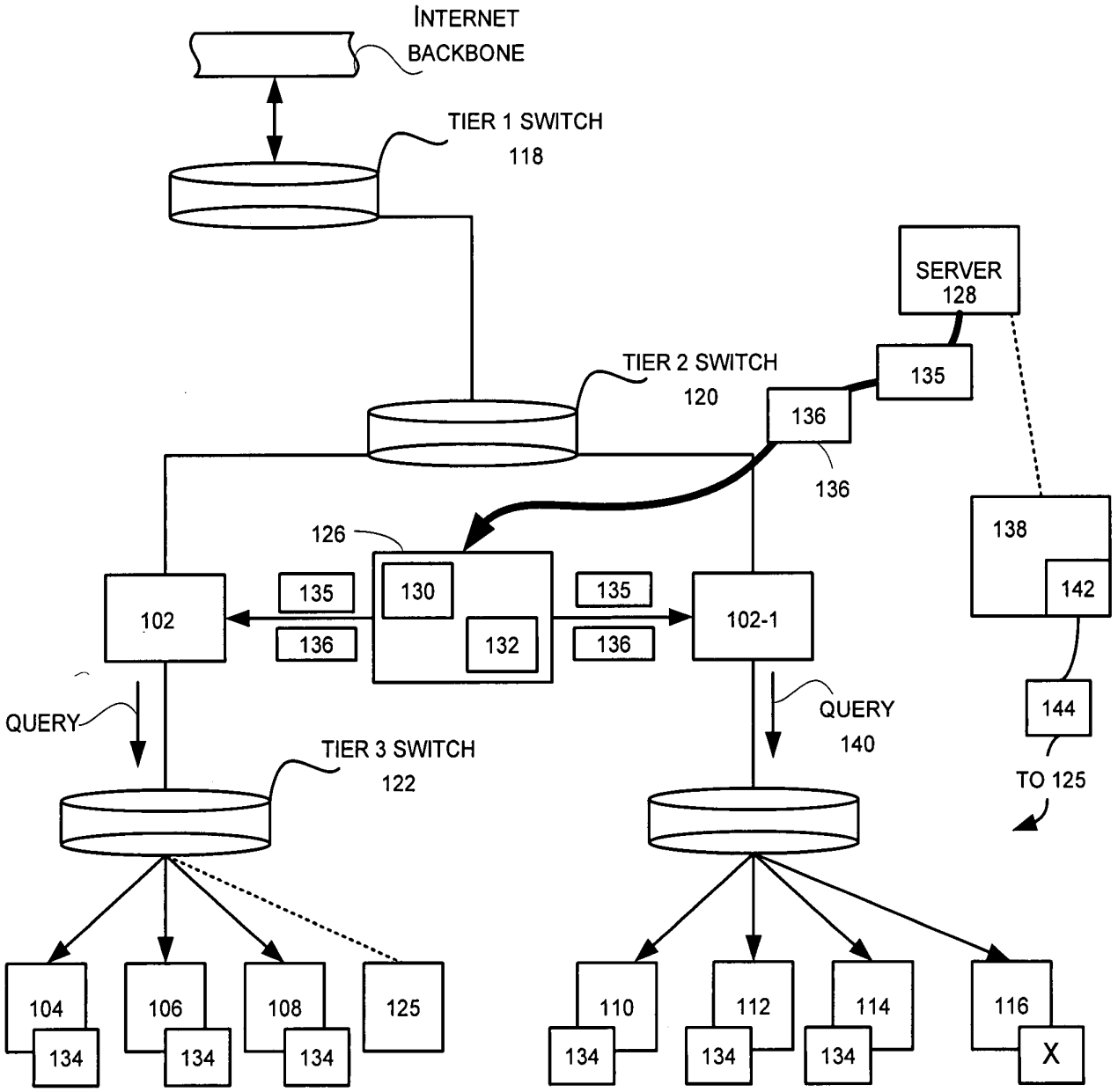

INTERNET BACKBONE
TIER 1 SWITCH 118
SERVER 128
TIER 2 SWITCH 120
UPDATES
100
126
130
132
102
102
CONTROLLER
TIER 3 SWITCH 122
TIER 3 SWITCH 122
104
106
108
125
110
112
114
116
134
134
134
134
134
134
134
134
VIRUS MONITORING SYSTEM



VIRUS MONITORING SYSTEM

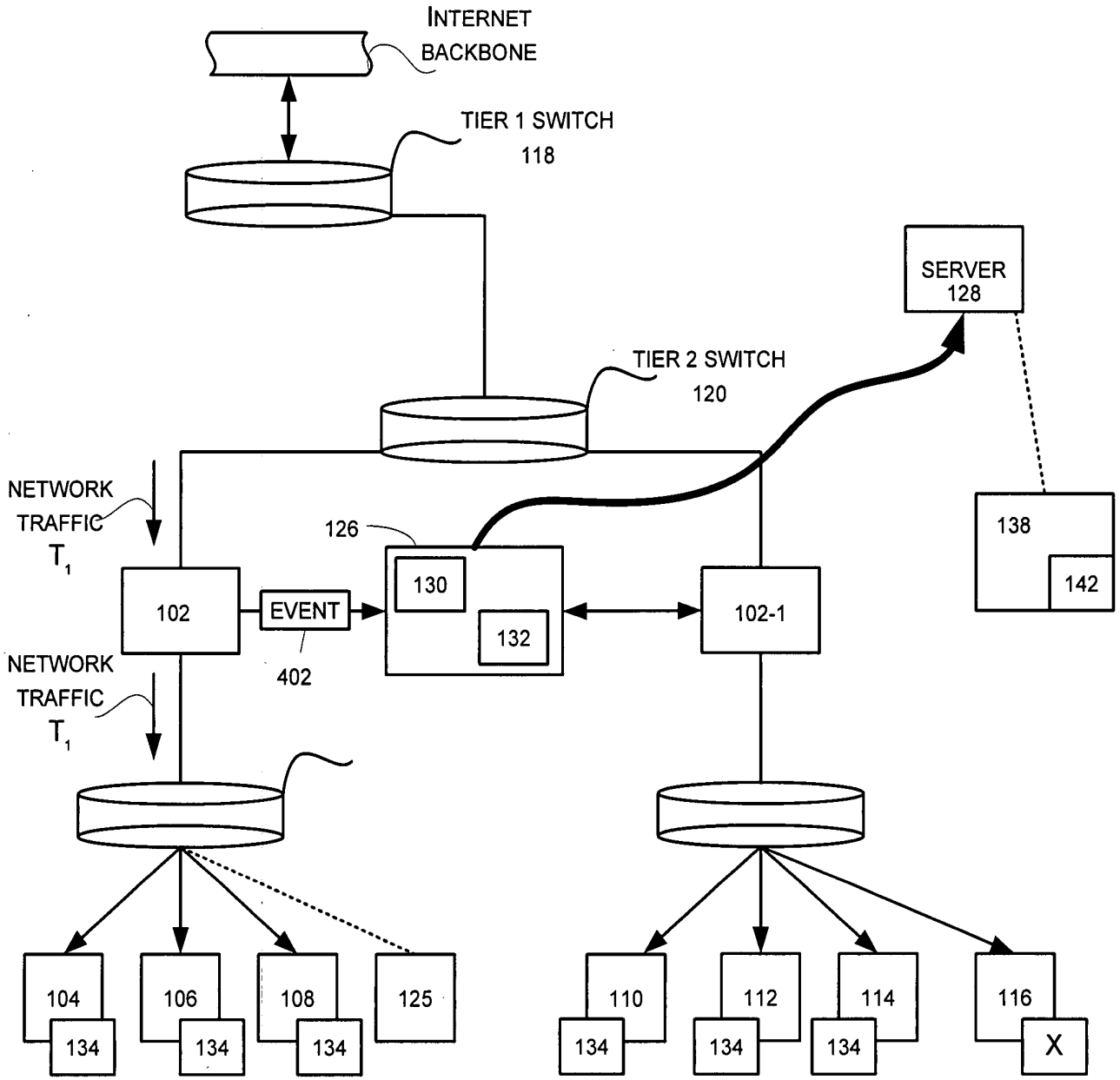
FIG. 2

FIG. 3



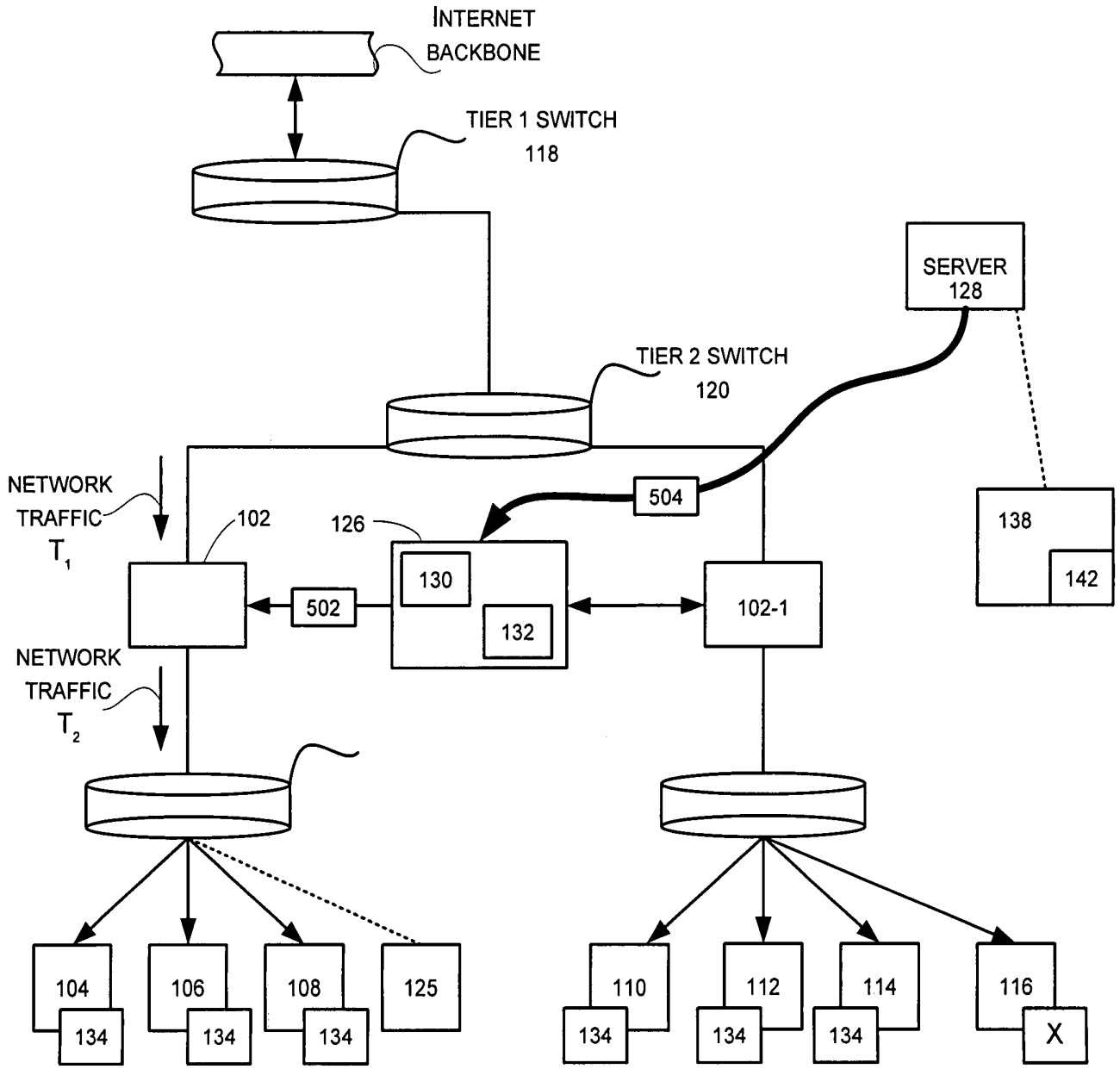
VIRUS MONITORING SYSTEM WITH VISITOR DEVICE

FIG. 4



VIRUS MONITORING SYSTEM - STANDBY MODE

FIG. 5



VIRUS MONITORING SYSTEM - STANDBY MODE

FIG. 6A

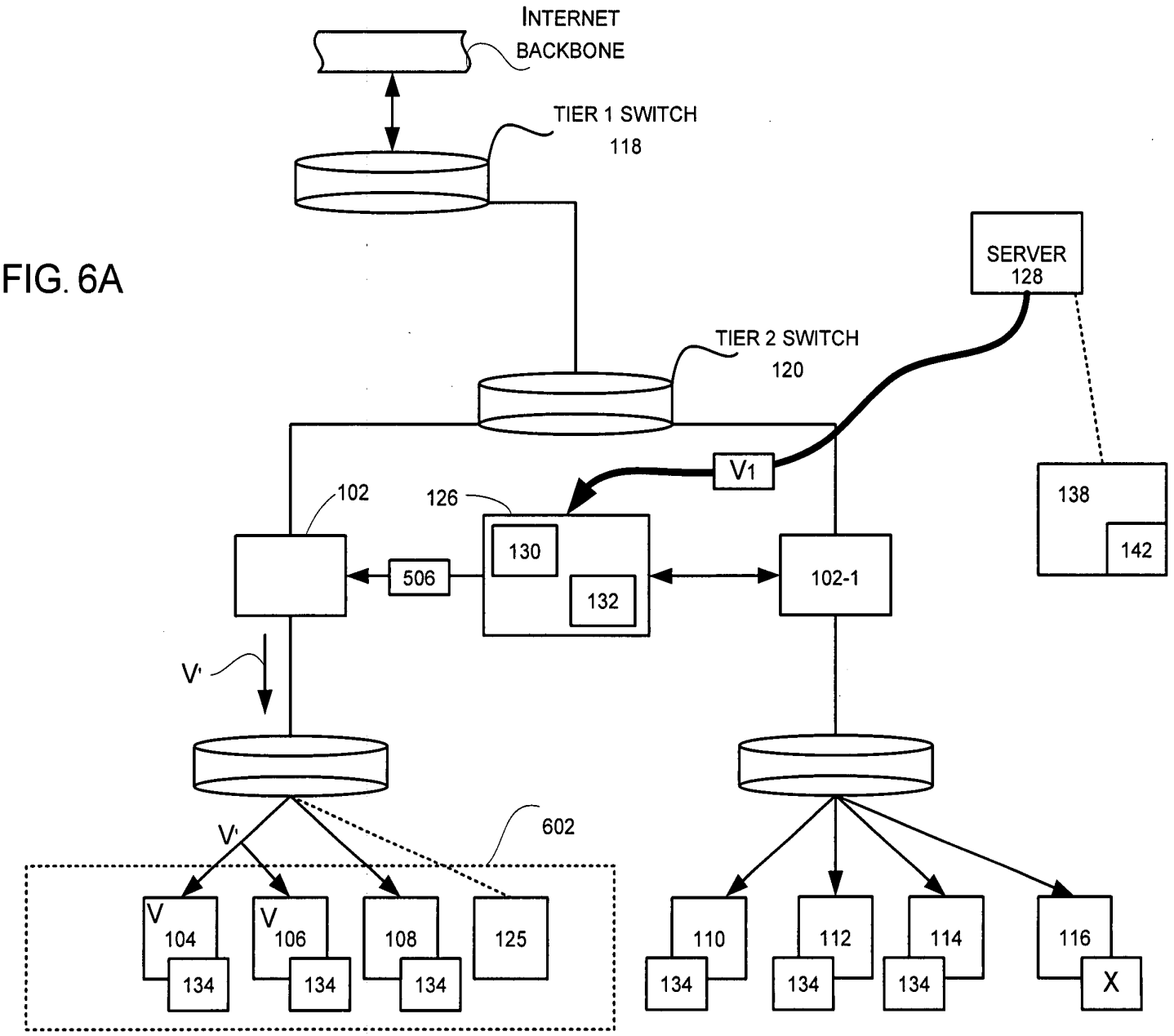
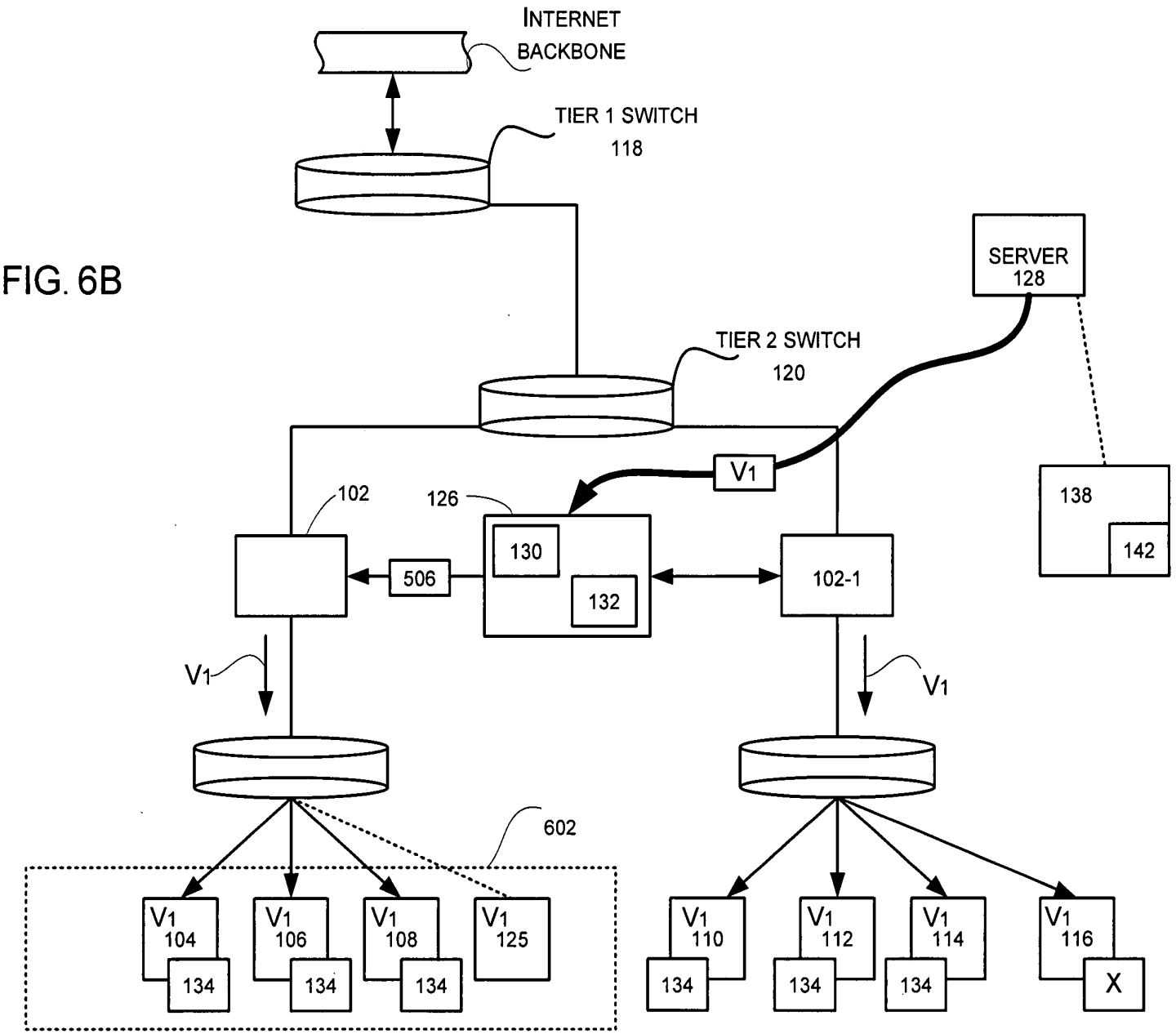

INTERNET
BACKBONE
TIER 1 SWITCH
118
SERVER
128
TIER 2 SWITCH
120
V1
102
126
130
132
506
102-1
138
142
V'
V'
602
V
104
134
V
106
134
108
134
125
110
134
112
134
114
134
116
X

FIG. 6B



VIRUS MONITORING SYSTEM - SEGMENT ISOLATION

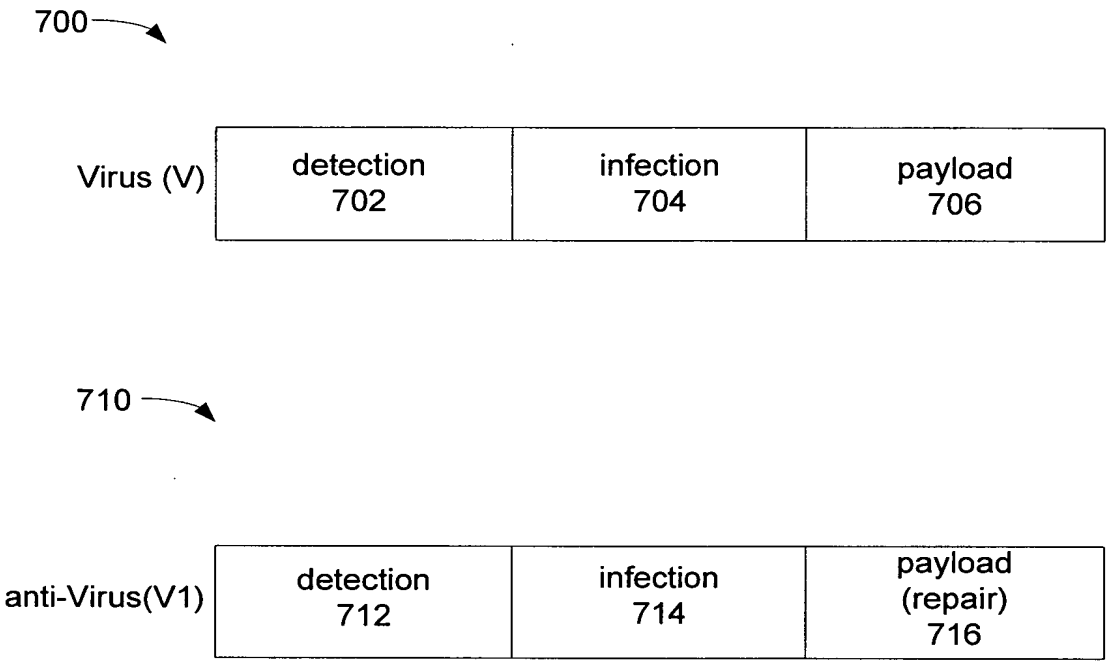

700
Virus (V)
detection
702
infection
704
payload
706
710
anti-Virus(V1)
detection
712
infection
714
payload
(repair)
716

FIG. 7

FIG. 8

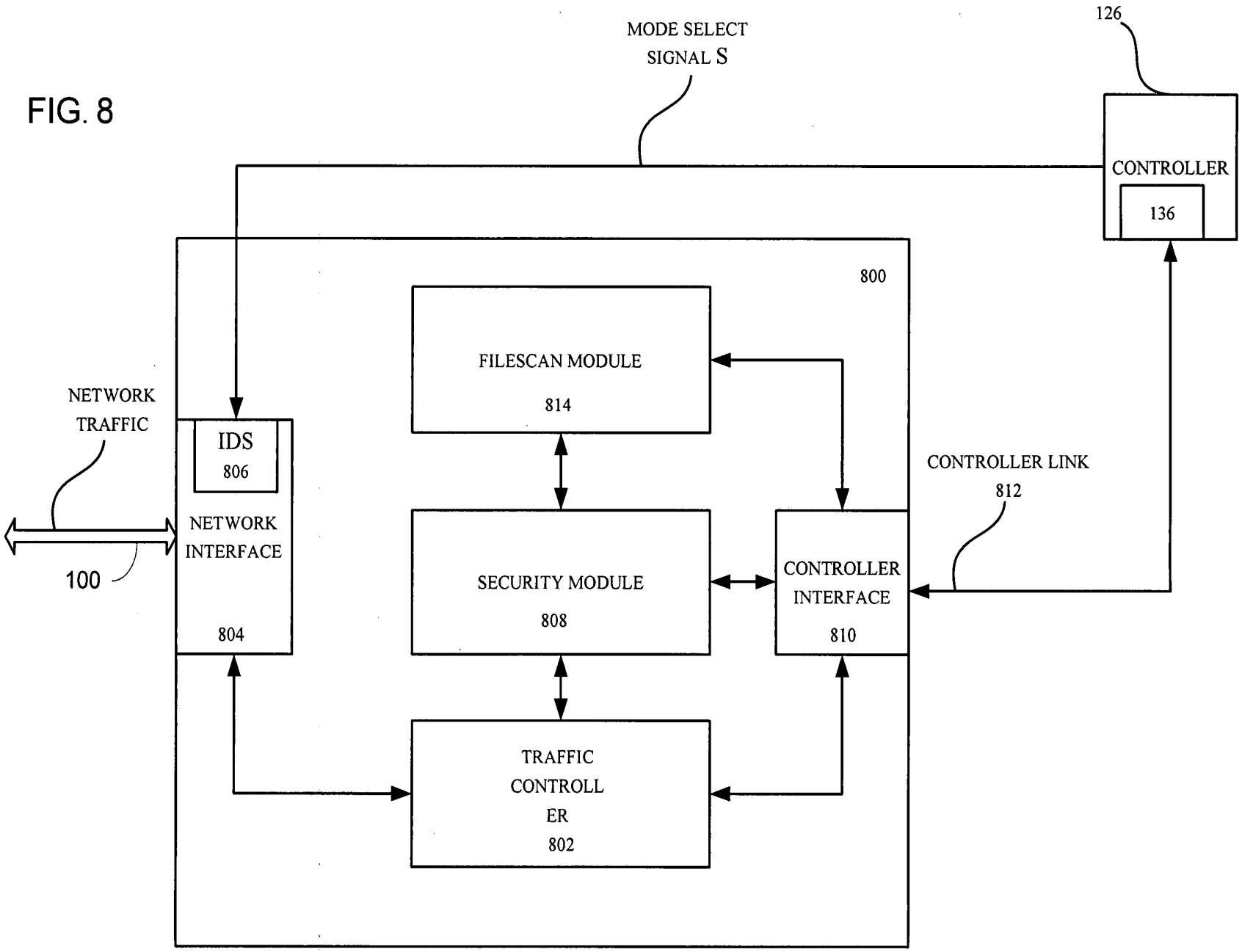
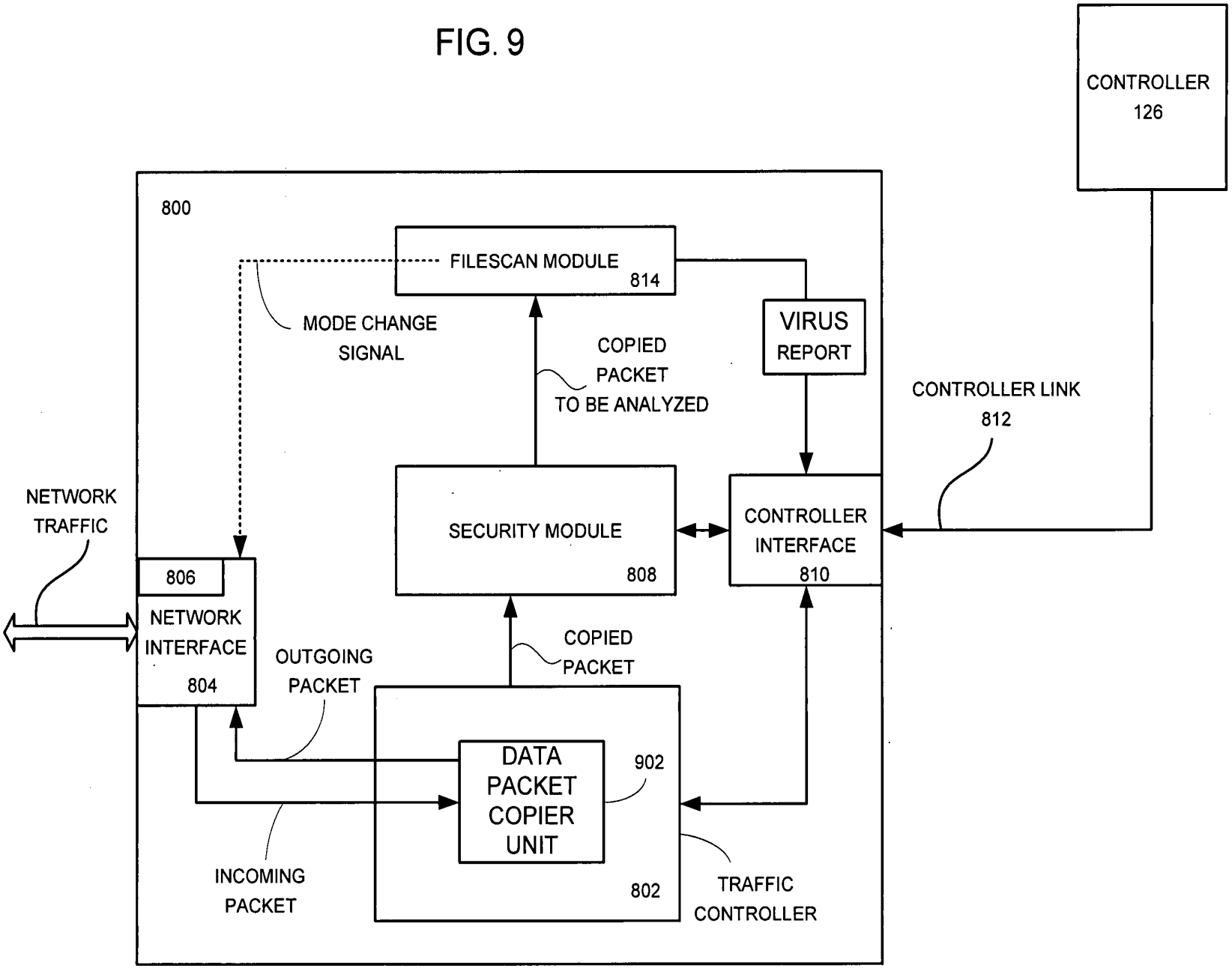

126
MODE SELECT
SIGNAL S
CONTROLLER
136
800
FILESCAN MODULE
814
NETWORK
TRAFFIC
IDS
806
NETWORK
INTERFACE
804
100
SECURITY MODULE
808
CONTROLLER LINK
812
CONTROLLER
INTERFACE
810
TRAFFIC
CONTROLL
ER
802

FIG. 9



VIRUS MONITOR - STANDBY MODE

FIG. 10

VIRUS MONITORING SYSTEM - STANDBY MODE

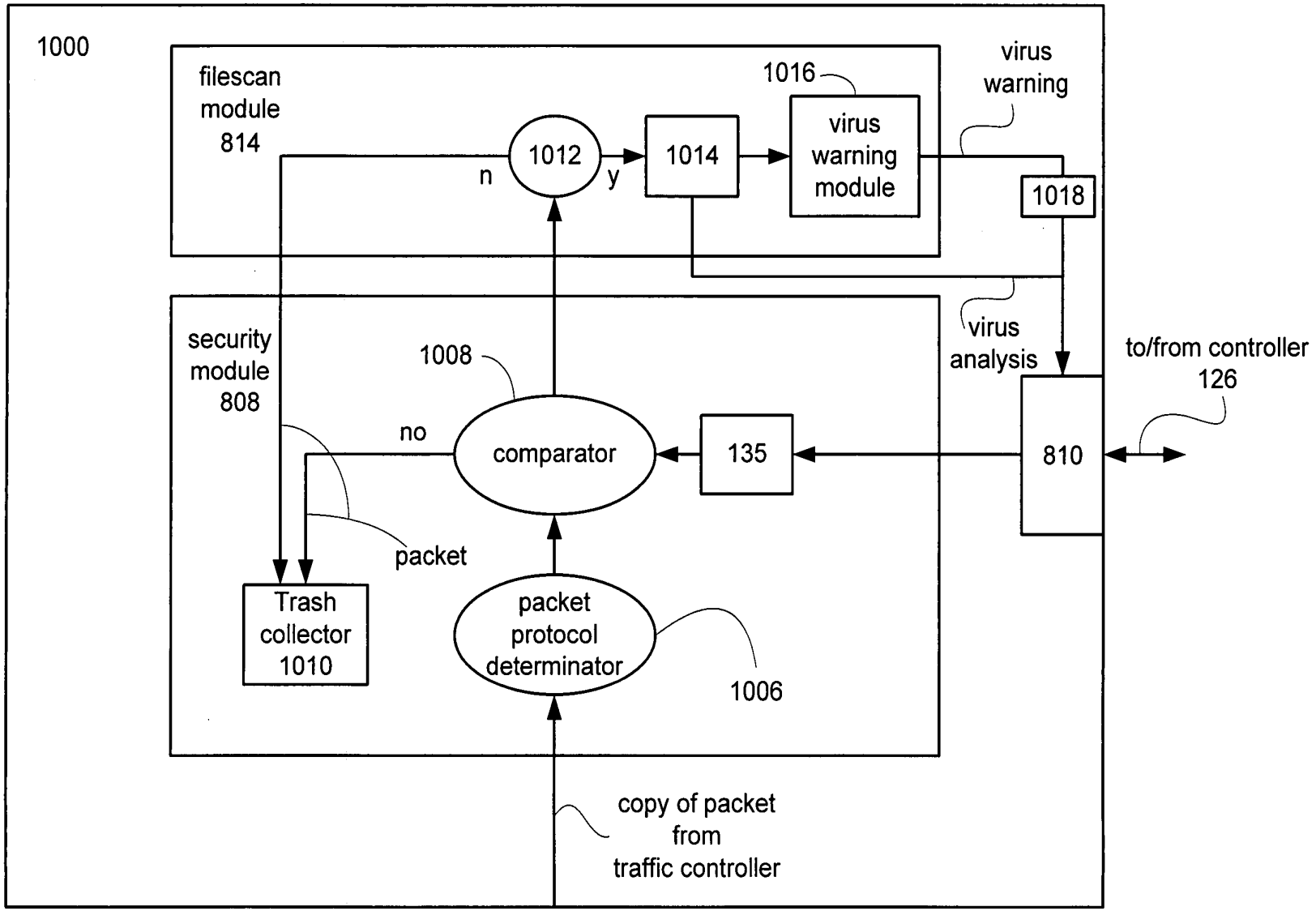
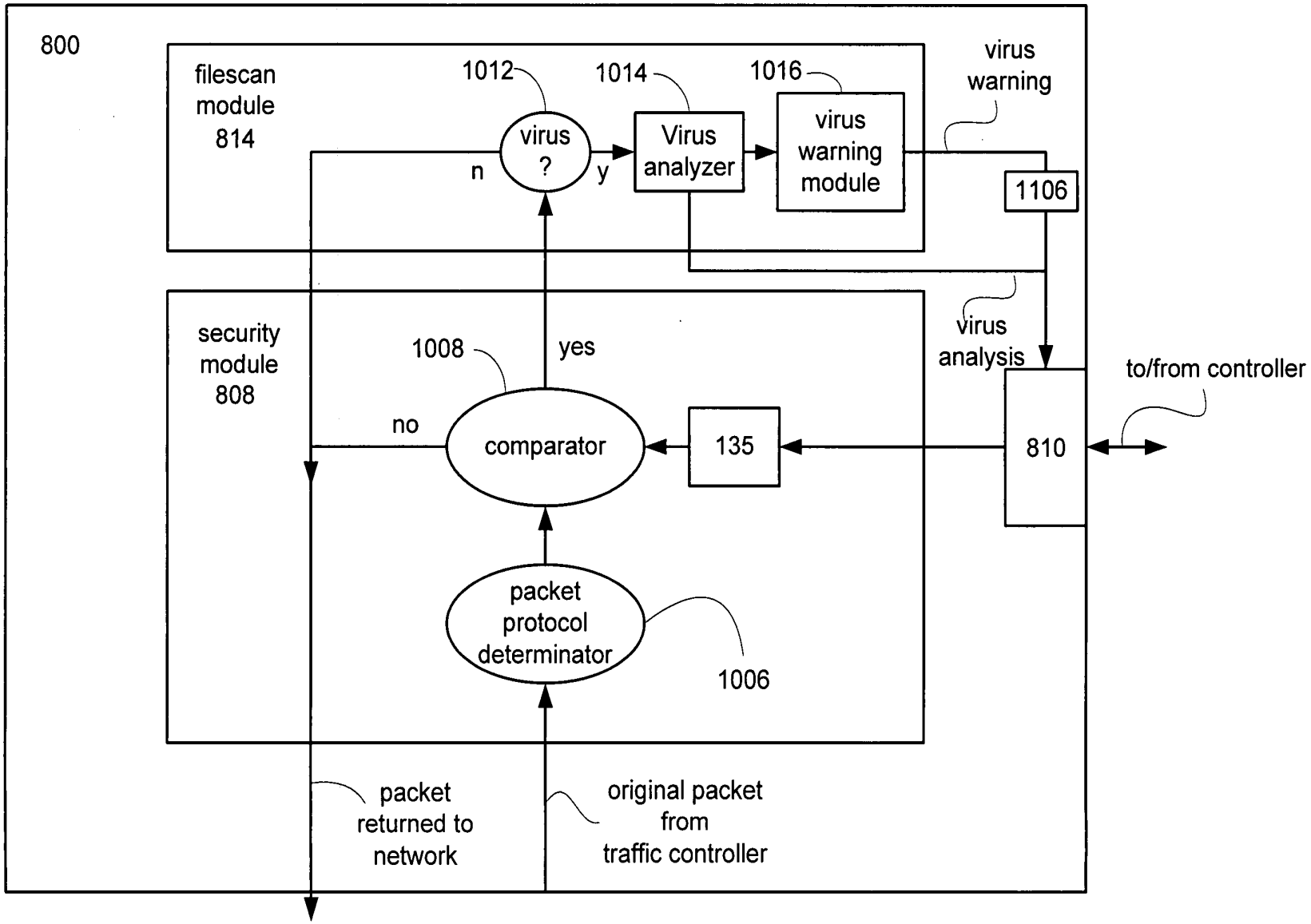


FIG. 11

VIRUS MONITORING SYSTEM - INLINE MODE



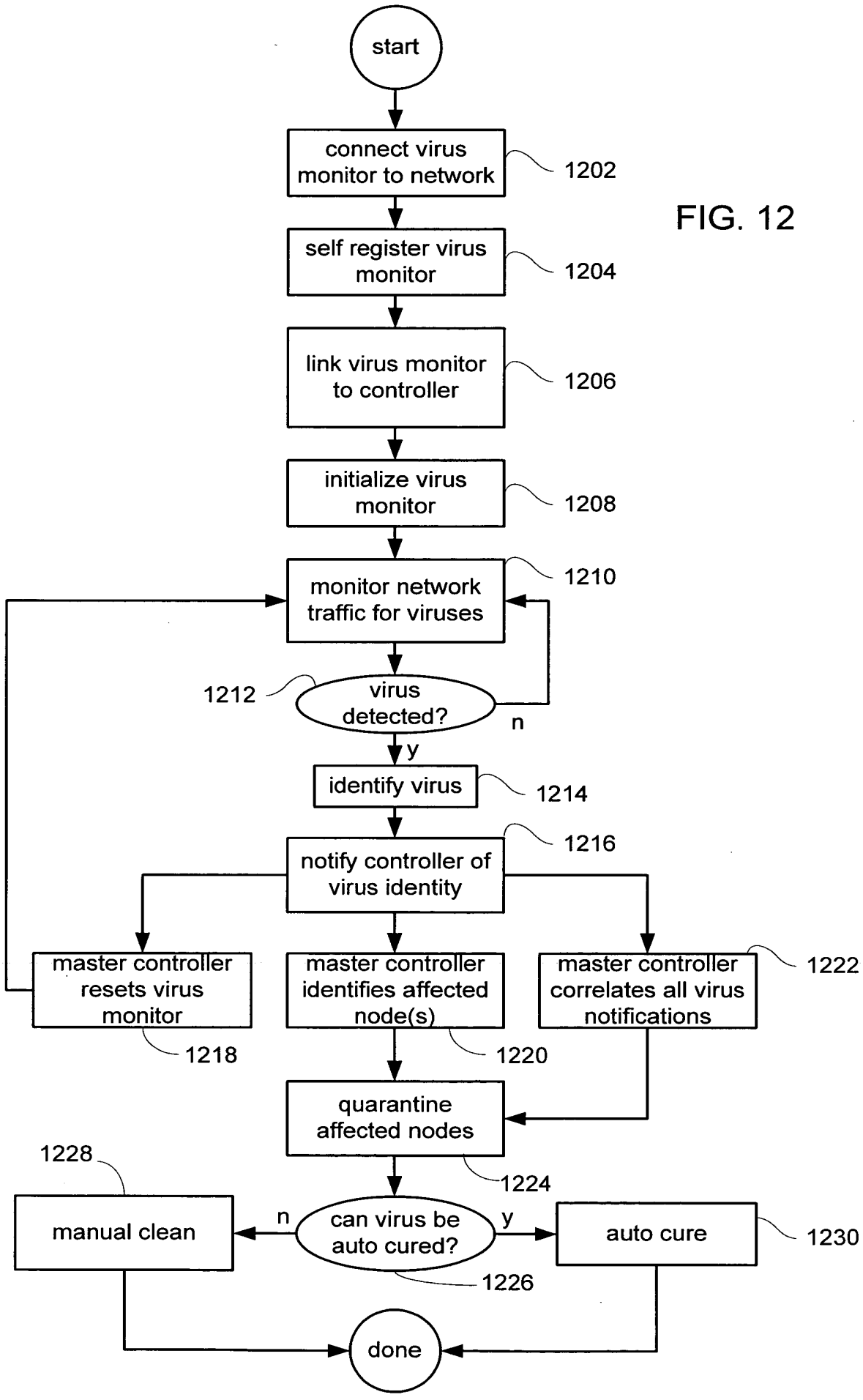

start
connect virus monitor to network
1202
self register virus monitor
1204
link virus monitor to controller
1206
initialize virus monitor
1208
monitor network traffic for viruses
1210
1212
virus detected?
n
y
identify virus
1214
notify controller of virus identity
1216
master controller resets virus monitor
1218
master controller identifies affected node(s)
1220
master controller correlates all virus notifications
1222
quarantine affected nodes
1224
1228
manual clean
n
can virus be auto cured?
y
auto cure
1230
1226
done

FIG. 12

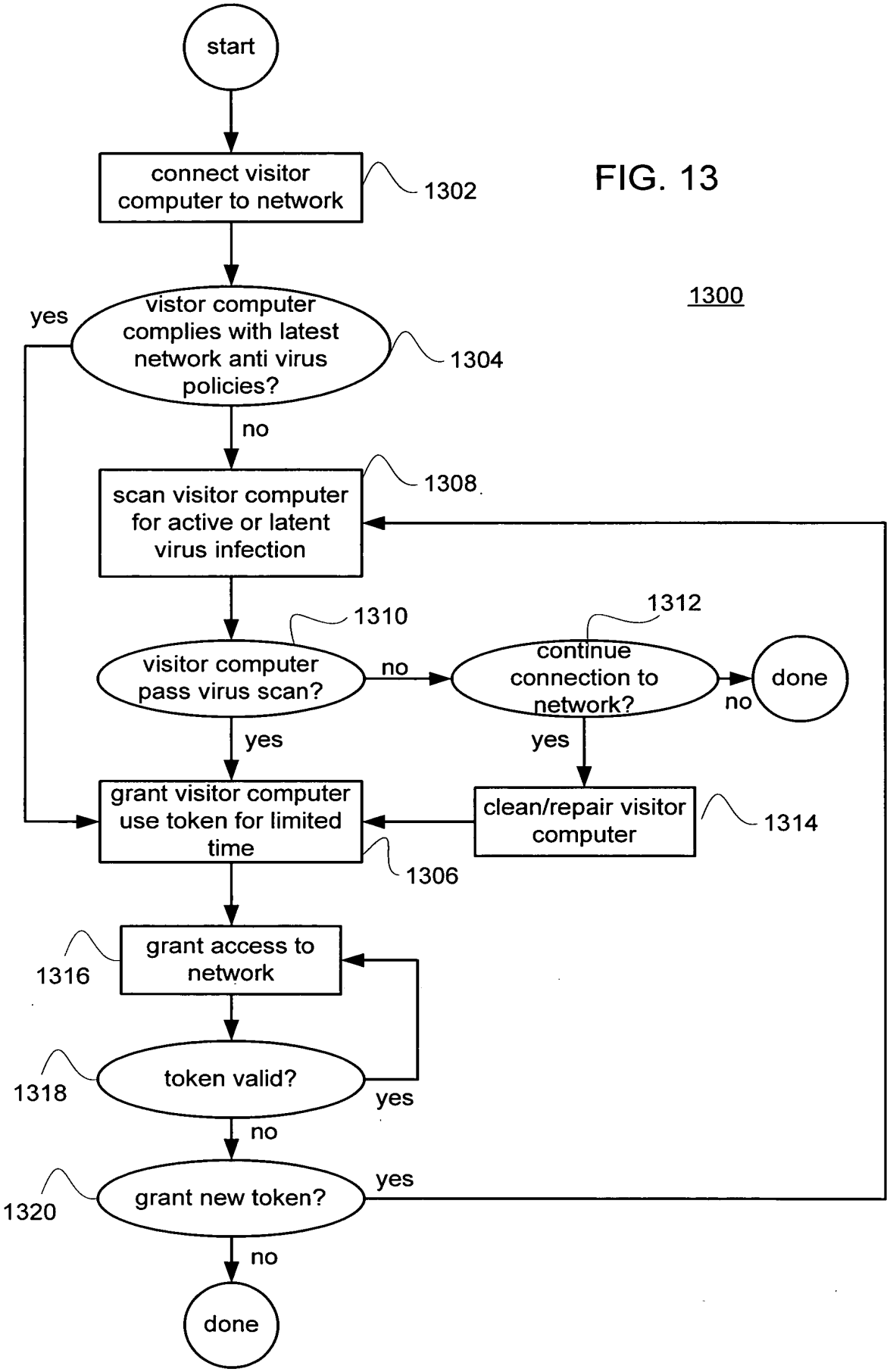
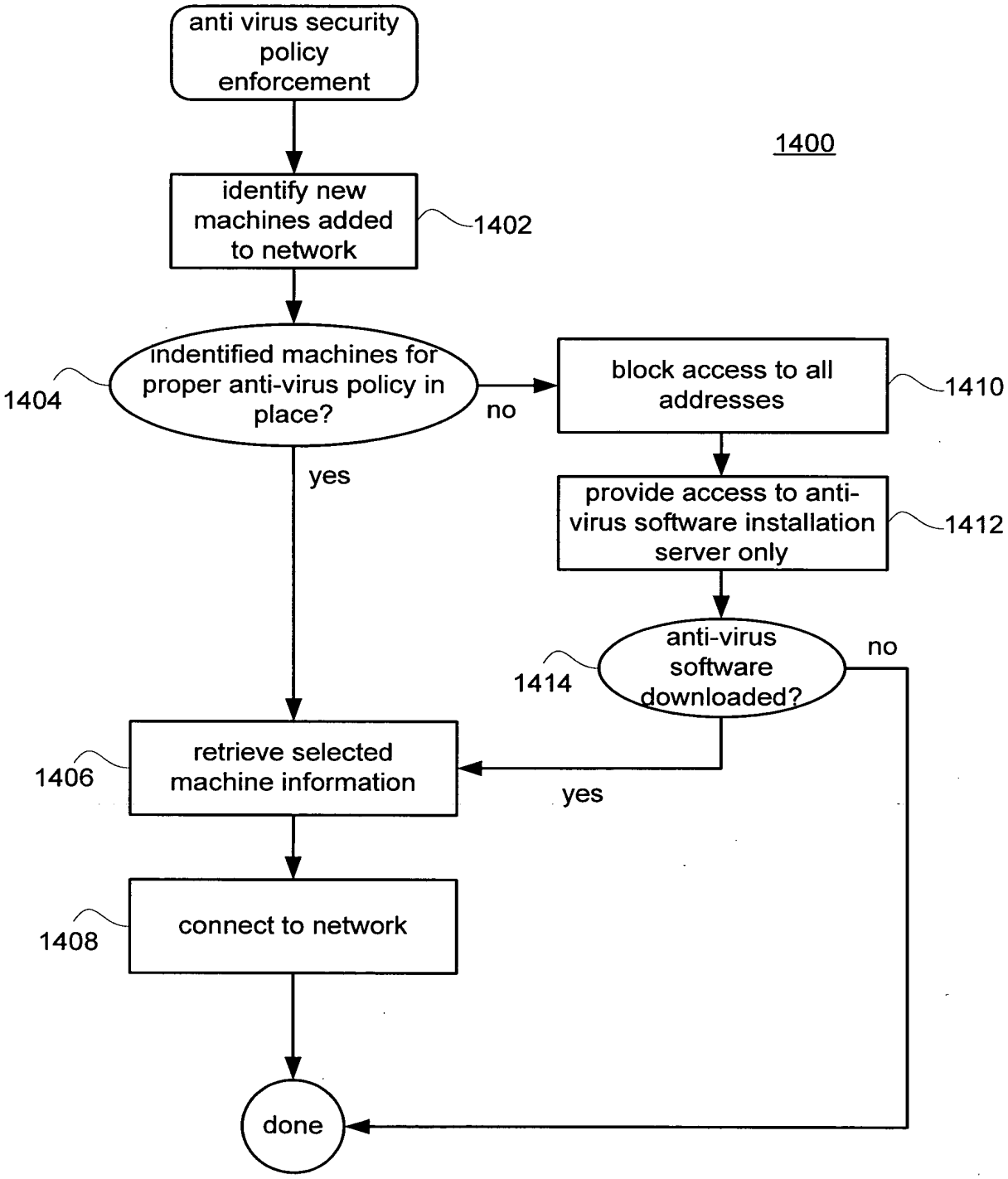

start
connect visitor computer to network
1302
vistor computer complies with latest network anti virus policies?
yes
1304
no
scan visitor computer for active or latent virus infection
1308
1310
visitor computer pass virus scan?
no
1312
continue connection to network?
done
no
yes
yes
grant visitor computer use token for limited time
clean/repair visitor computer
1314
1306
grant access to network
1316
token valid?
1318
yes
no
grant new token?
yes
1320
no
done

FIG. 13

1300

Fig. 14


anti virus security policy enforcement
1400
identify new machines added to network
1402
indentified machines for proper anti-virus policy in place?
1404
no
block access to all addresses
1410
yes
provide access to anti-virus software installation server only
1412
anti-virus software downloaded?
1414
no
yes
retrieve selected machine information
1406
connect to network
1408
done

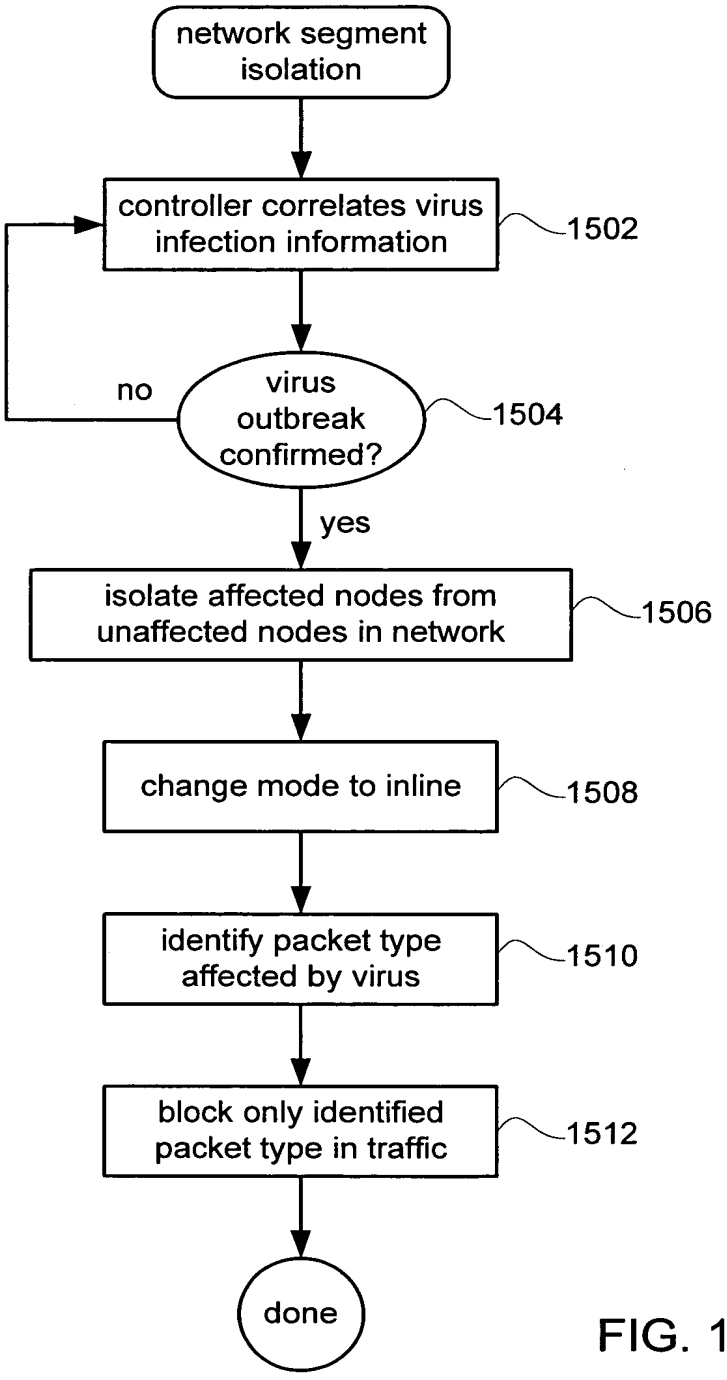

network segment isolation
1500
controller correlates virus infection information
1502
no
virus outbreak confirmed?
1504
yes
isolate affected nodes from unaffected nodes in network
1506
change mode to inline
1508
identify packet type affected by virus
1510
block only identified packet type in traffic
1512
done

FIG. 15

FIG. 16

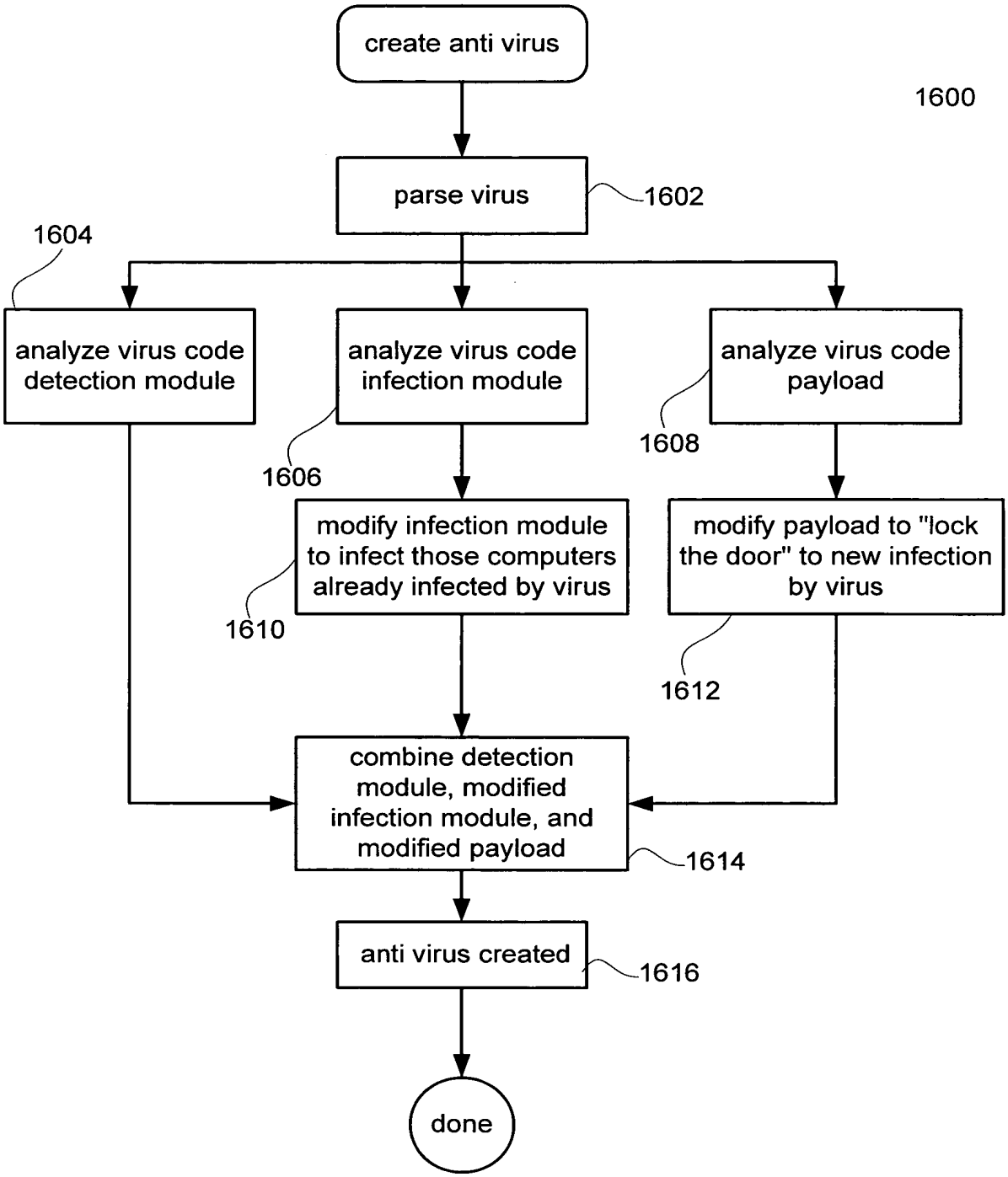

create anti virus
1600
parse virus
1602
1604
analyze virus code detection module
analyze virus code infection module
analyze virus code payload
1606
1608
modify infection module to infect those computers already infected by virus
modify payload to "lock the door" to new infection by virus
1610
1612
combine detection module, modified infection module, and modified payload
1614
anti virus created
1616
done

FIG. 17

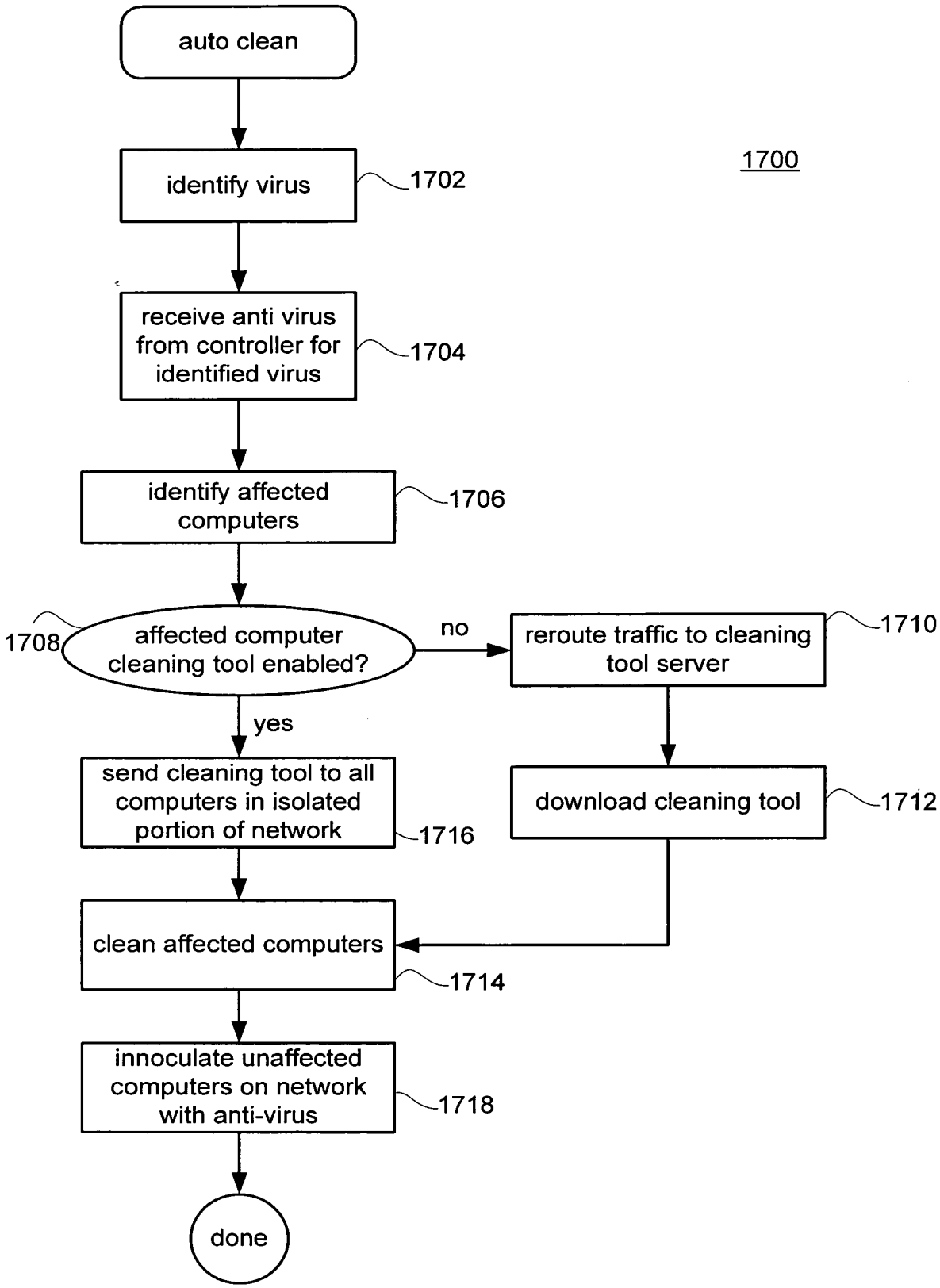
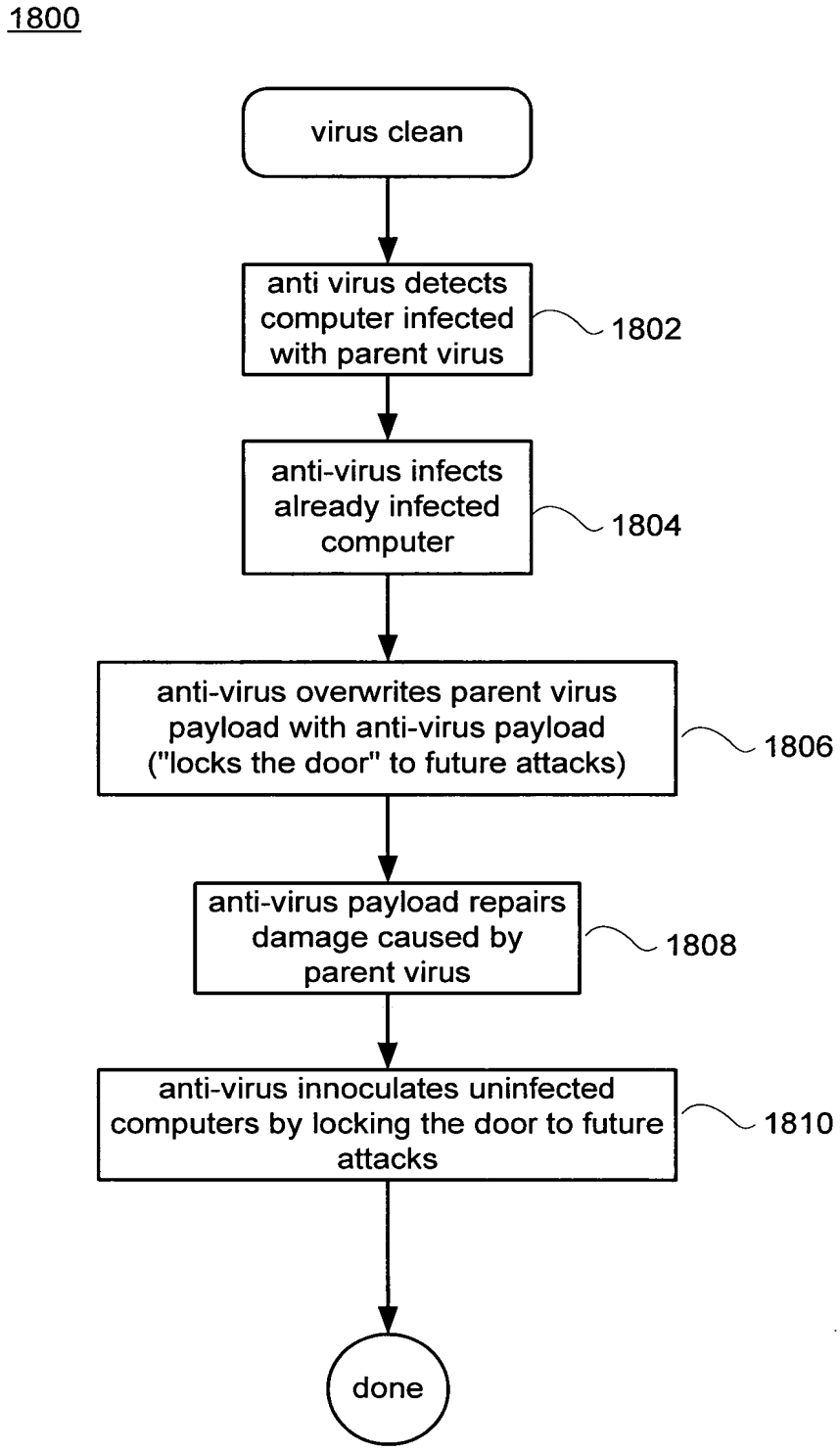
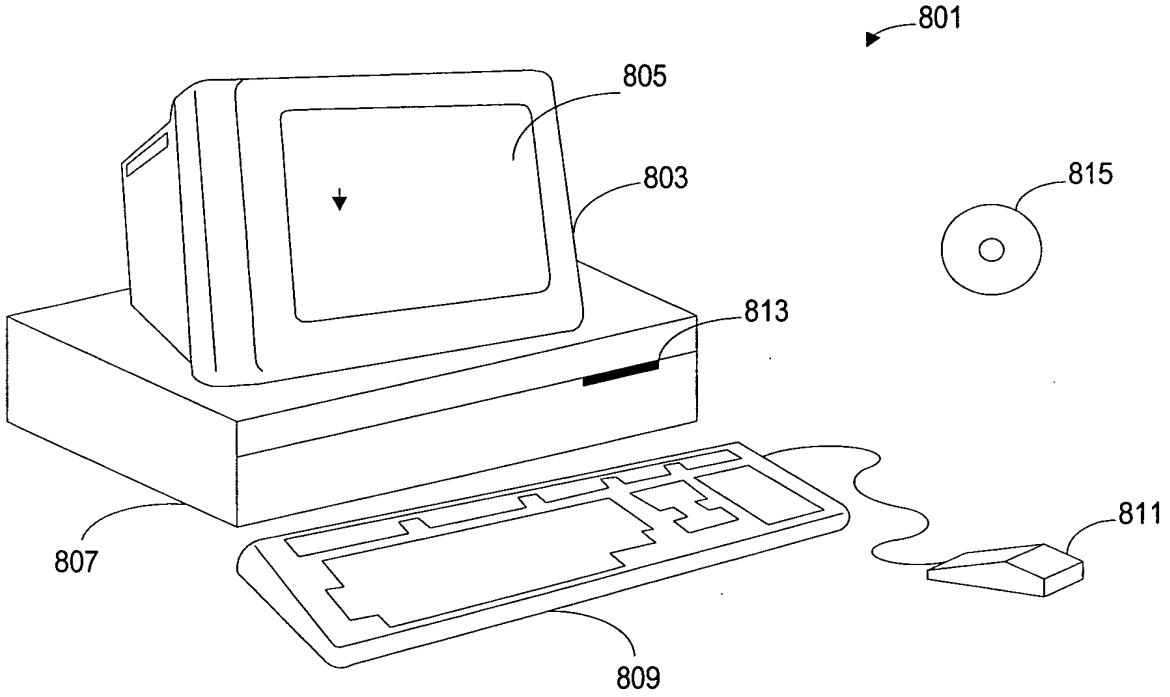

auto clean
identify virus
1702
receive anti virus from controller for identified virus
1704
identify affected computers
1706
1708
affected computer cleaning tool enabled?
no
reroute traffic to cleaning tool server
1710
yes
send cleaning tool to all computers in isolated portion of network
1716
download cleaning tool
1712
clean affected computers
1714
innoculate unaffected computers on network with anti-virus
1718
done
1700

FIG. 18


1800
virus clean
anti virus detects computer infected with parent virus
1802
anti-virus infects already infected computer
1804
anti-virus overwrites parent virus payload with anti-virus payload ("locks the door" to future attacks)
1806
anti-virus payload repairs damage caused by parent virus
1808
anti-virus innoculates uninfected computers by locking the door to future attacks
1810
done


801
805
803
815
813
811
807
809

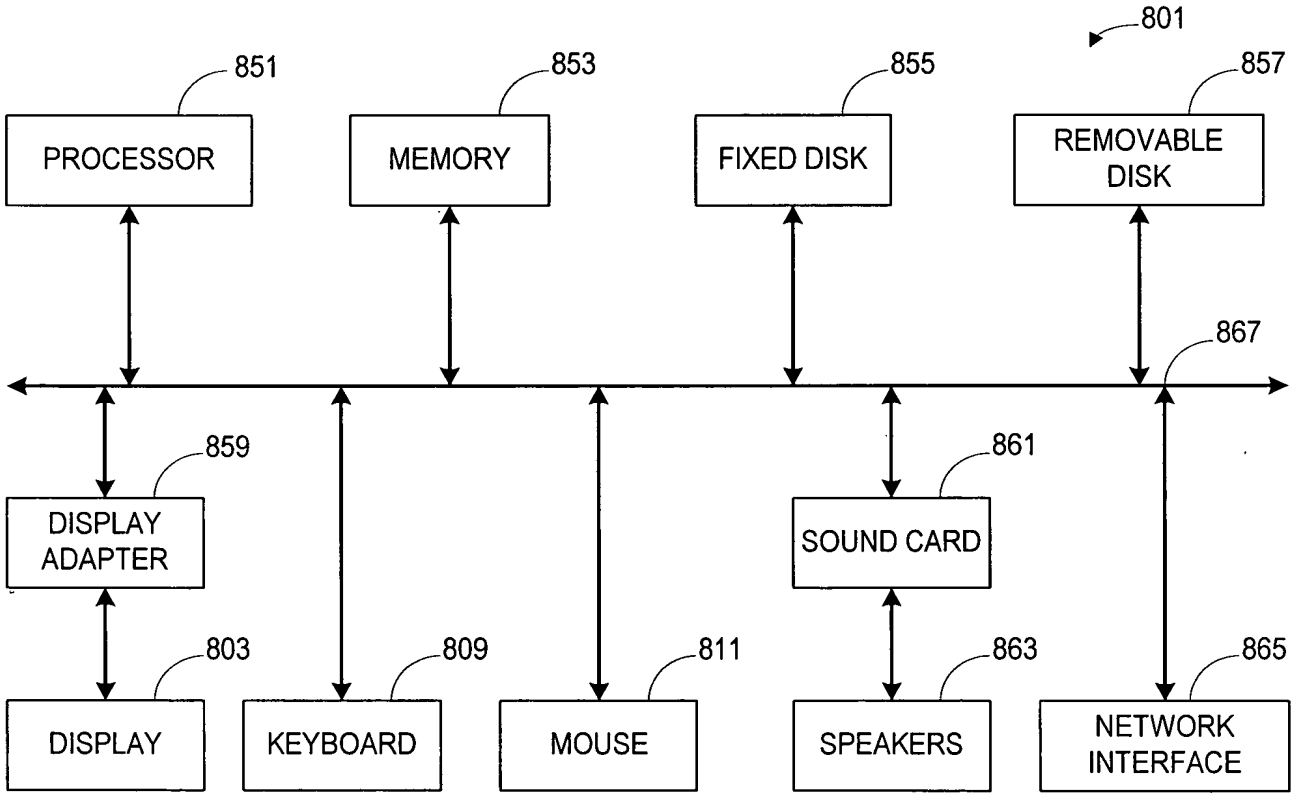

801
851
853
855
857
PROCESSOR
MEMORY
FIXED DISK
REMOVABLE DISK
867
859
861
DISPLAY ADAPTER
SOUND CARD
803
809
811
863
865
DISPLAY
KEYBOARD
MOUSE
SPEAKERS
NETWORK INTERFACE

FIG. 19